Published on *The National Law Review* https://www.natlawreview.com

FTC Blog: “The FTC Act Creates a De Facto Breach Disclosure Requirement”

Article By:

Joseph J. Lazzarotti

On May 20, 2022, the Federal Trade Commission’s Team CTO and the Division of Privacy and Identity Protection published a blog post entitled, “Security Beyond Prevention: The Importance of Effective Breach Disclosures.” In the post, the FTC takes the position that in some cases there may be a de facto data breach notification requirement, despite there currently being no section of the Federal Trade Commission Act or implementing regulation imposing an express, broadly applicable data breach notification requirement. Businesses should nonetheless take this de facto rule into account as part of their incident response plans.

The post stresses the importance of strong incident detection and response processes, noting they are vital to maintaining reasonable security. The notification component can prevent and minimize consumer harm from breaches because, among other things, it can spur consumers to take actions to mitigate harm resulting from the breach. According to the FTC, failure to maintain such practices could indicate a lack of competition in the marketplace. Notably, the post states:

> "Regardless of whether a breach notification law applies, a breached entity that fails to disclose information to help parties mitigate reasonably foreseeable harm may violate Section 5 of the FTC Act."

The American Recovery and Reinvestment Act of 2009 directed the FTC to establish rules to require notification to consumers when the security of their individually identifiable health information has been breached. However, those rules apply only to vendors of personal health records and related entities, although a recent FTC policy statement clarified the application of the rule. In support of the blog post’s more broadly applicable de facto requirement, the FTC discussed some recent enforcement actions.

The post referred to the recent settlement with an online retailer that allegedly failed to timely notify consumers and other relevant parties after data breaches, thereby preventing parties from taking measures to mitigate harm. The FTC viewed this as an unfair trade practice. Looking to other enforcement actions as examples, the post explained that deceptive statements can hinder

consumers from taking critical actions to mitigate foreseeable harms like identity theft, loss of sensitive data, or financial impacts. Looking at these cases together, the post concluded that:

> "companies have legal obligations with respect to disclosing breaches, and that these disclosures should be accurate and timely."

As any victim of a data incident or experienced breach counsel knows, a critical part of just about any security incident is determining whether there has been a breach and whether notification is required. For an incident affecting individuals in a significant number of countries and/or states, navigating the various data breach statutes and regulations is challenging. According to the FTC's post, even if that process leads to the conclusion that notification is not required under state law, for example, the FTC's de facto rule may apply to avoid an allegation of unfair or deceptive trade practice.

Business, therefore, should review their incident response plans in light of this informal guidance.

National Law Review, Volumess XII, Number 143